João Pedro Fernandes Reis

1. Faça um breve relatório descrevendo como o processo de criptografia assimétrica foi aplicado na criação do certificado digital autoassinado.

Primeiramente foi gerada uma chave privada para assinar digitalmente os arquivos.

Segundamente geramos um arquivo .csr com as informações necessárias para gerar um certificado digital.

Em terceiro lugar executamos o comando para gerar um certificado digital assinado pela chave privada gerada e com as informações do arquivo .csr.

Após tudo isso podemos gerar um arquivo pfx que é o arquivo de instalação do certificado digital no Windows.

2. Explique o que é um certificado autoassinado e qual a sua aplicabilidade.

Esse tipo de certificado serve para assinar arquivos, ou seja, com esse certificado instalado no Windows será possível assinar documentos e as informações contidas nesse certificado serão mostradas no arquivo assinado, podendo verificar a autenticidade do mesmo.

3. Como seria o processo de validação do certificado digital criado?

Um sistema de verificação de certificado iria pegar a chave pública armazenada nos metadados do documento, decriptografar o hash armazenado na assinatura e verificar se o hash bate com o hash atual do arquivo assinado, se bater, significa que a integridade do arquivo não foi alterada.

4. Qual o tipo de certificado digital criado?

O tipo do certificado gerado é o A1, é um tipo de certificado que dura 365 dias normalmente, pois por ser digital o ideal é que não dure muito. Ele serve para assinar documentos digitalmente.